Nuclear Plant Risk Assessment

Jeffrey Mahn

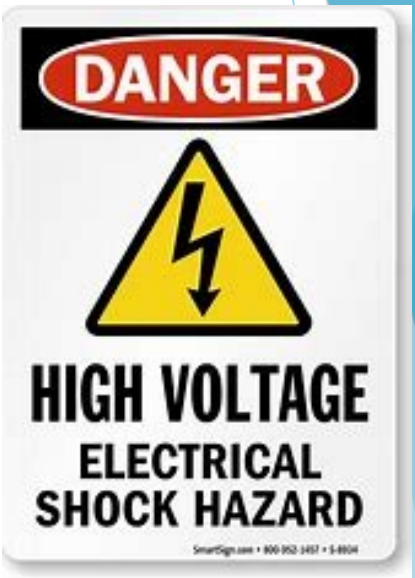
Nuclear Engineer (Retired)

jamahn47@gmail.com

Hazard and Risk

Hazard – something with potential to cause harm

Risk – likelihood of harm occurring



Principles of Risk Management

- Everything has hazards; all hazards have risk
- Risks not equally consequential
- Two components of risk – consequence severity and probability of occurrence; both must be evaluated to assess risk
- Humans lack omniscience – some risks will not be known
- Humans lack precognition – some risks will not be foreseen
- Human resources limited – resources available to control risks also limited
- Something is “safe” only to degree that its risks are acceptable; no absolute safety
- Recognized risks exceeding acceptability limit must be made known to those who may suffer their consequences

Principles of Risk Management (cont.)

- Probabilities of all risks are finite; bizarre (low probability) mishap **will** occur – sometime, somewhere
  - Risk probability calculations, although necessary for performing bona fide risk assessments, must not be afforded absolute status
  - Extremely low probability event can happen today, tomorrow, or next week
  - Extremely low probability event could even happen today, tomorrow, and next week; not likely, but neither are other unlikely catastrophes that strike without any apparent schedule (e.g., earthquakes and floods)

Risk Management Maxims

Risk Issues are Emotional

Solutions are Technical

Decisions are Political

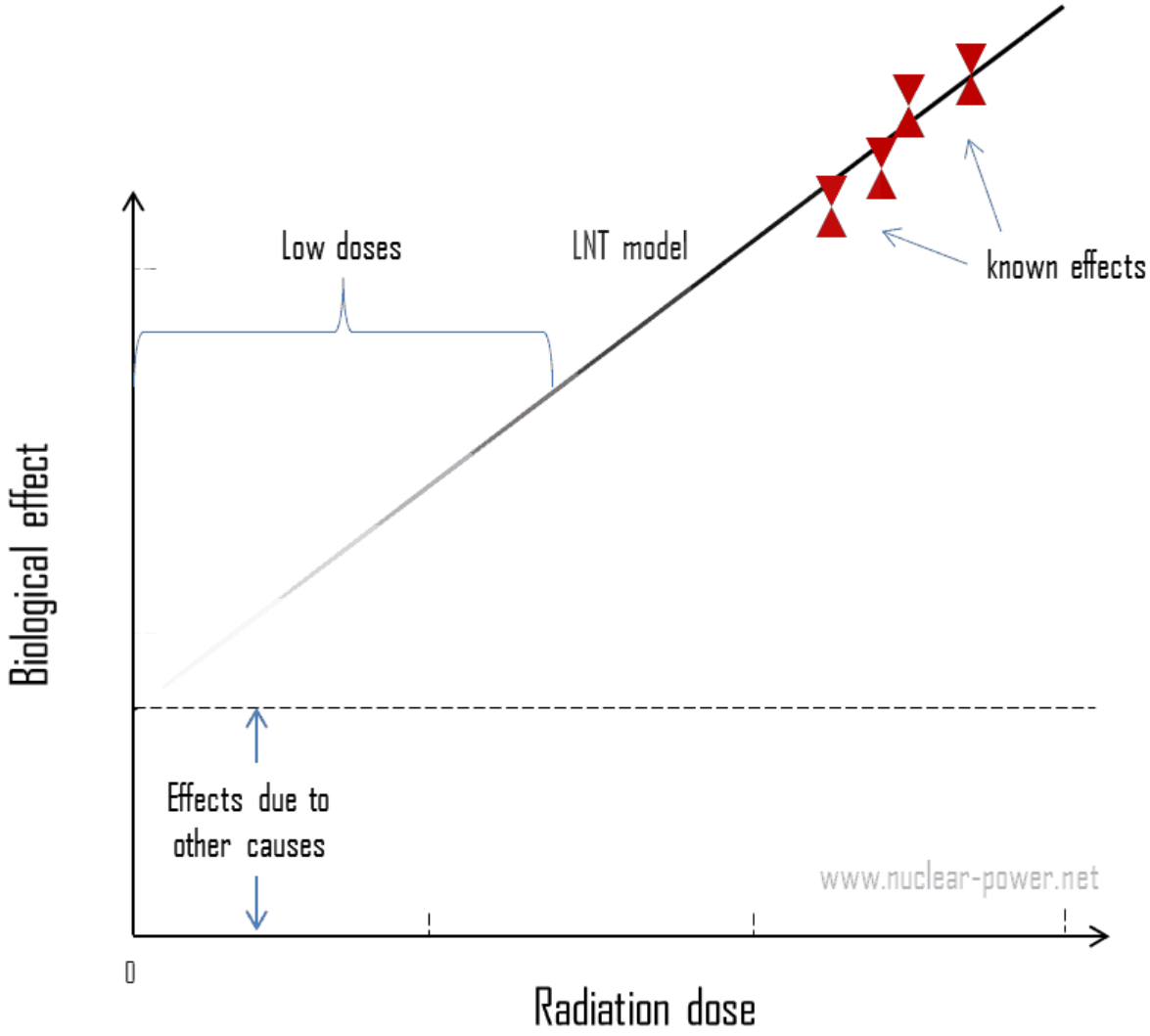
Risk Perception

- Most significant influence on public's understanding of risk
- Generally driven more by magnitude of potential consequences, even for extremely low likelihoods of occurrence
- Complex technologies like nuclear power assumed by public to have much higher risks than warranted
- Major obstacle to effective risk communication
  - Disagreement with notion that some risks are "acceptable"
  - Discussions of what should be considered acceptable level of risk often raise high emotional passions

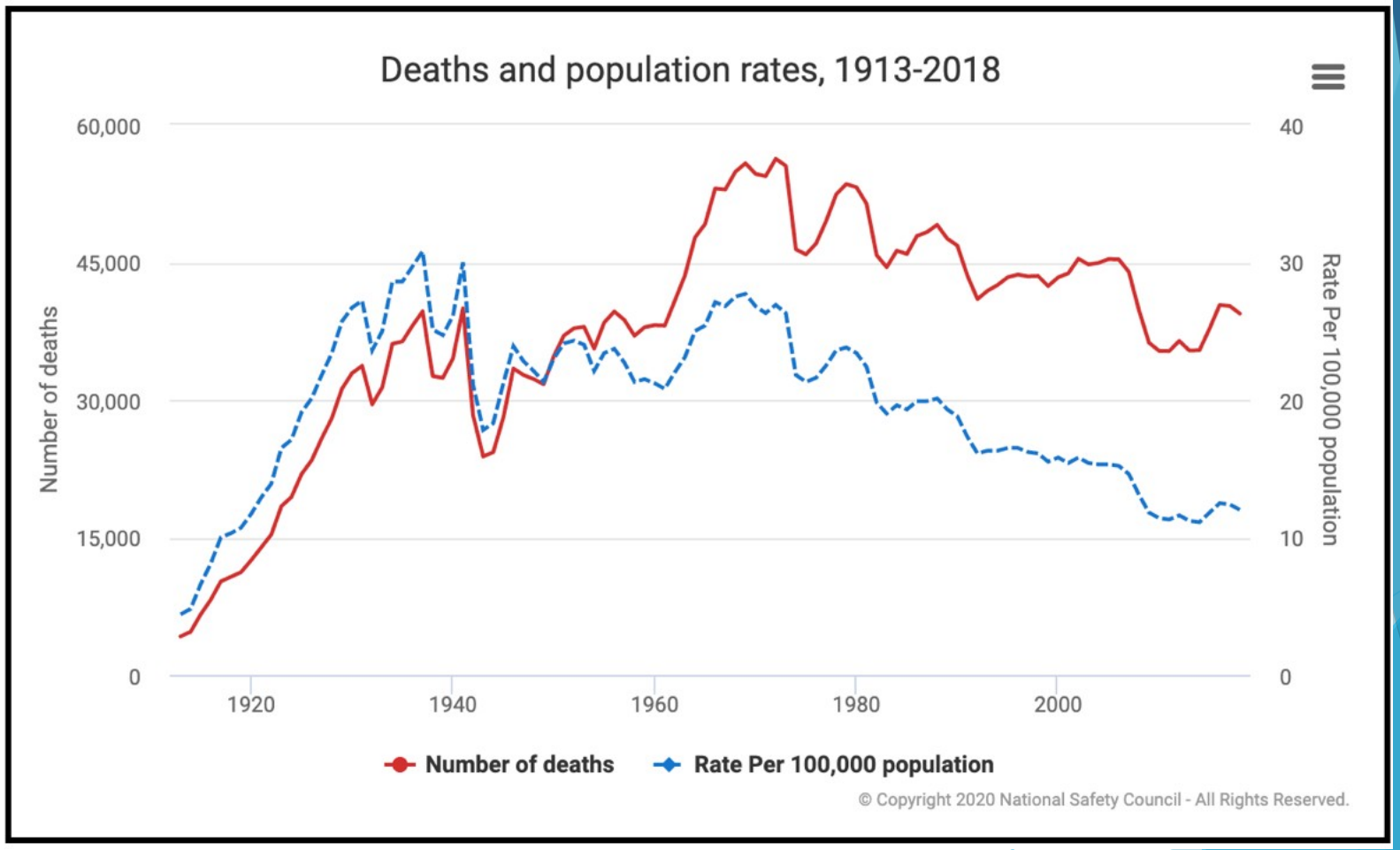
Risk Models

- Theoretical risk model based on limited data; heavily reliant on assumptions, inference, and extrapolation, often resulting in
  - risk hierarchy based on emotion-laden risk perceptions
  - mitigation strategies focused on agenda-based risk symptoms
  - decision–making driven by ideology resulting in either no risk mitigation or unacknowledged transfer of risk
- Data-based risk model based on empirical data accumulated from real world events that render
  - risk hierarchy based on logical, analytical thinking
  - mitigation strategies focused on identifying and resolving root causes of risk
  - decision-making aided by informed and knowledgeable experts

Theoretical Risk - LNT Model



Data-based Risk – U.S. Motor Vehicle Fatalities



Unacceptable Transfer of Risk

One experienced radiation health specialist told of his transition from being a compliant LNT supporter to being opposed to its continued use as the basis for regulations and decisions. He was in charge of a cleanup at a Pacific atoll that was contaminated to a level at which a population of 1000 living on the island for 40 years *might* experience one extra cancer death (based on LNT model prediction).

He told how he had to bring four members of his cleanup crew home in body bags because they had been killed in the kinds of accidents that are common in heavy construction and earthmoving operations. The cleanup also resulted in approximately 54 lost time accidents. He said he “hated the LNT” because of the way it transferred risk from hypothetical, computed harms to real harm to real people.

Risk Communication

- Generally, no distinction made between theoretical risk and real risk when communicating risk matters to public
- Potential consequences of theoretical risks heavily dependent on assumptions underlying risk model; generally, not addressed in public risk communications
- Faulty or biased communications often responsible for misunderstanding of risk issues by public
  - Media generally guilty of communicating unwarranted dire speculations and outright falsehoods about undesired events before facts are available
  - Media often directs “poor risk communication” allegations at those assumed to be responsible for undesired events

How Risk Expressed

- Risk mostly relative quantity that's rather meaningless unless compared to values from other events, or for same event over different time interval
- Safety risk generally expressed as combination of likelihood of hazard occurrence and hazard consequence in form of risk matrix
  - Qualitative risk assessments – likelihood of occurrence axis provided with labels such as Unlikely, Possible, and Likely, while consequence axis provided with labels such as Major, Moderate, and Minor
  - Quantitative risk assessments – each likelihood label defined by range of hazard frequencies (e.g., probability per year) and each consequence label defined by severity of possible hazard outcomes (e.g., million-dollar financial loss)

Example Qualitative Risk Matrix

		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
Consequences	5 Catastrophic	5 Moderate	10 High	15 Extreme	20 Extreme	25 Extreme
	4 Major	4 Moderate	8 High	12 High	16 Extreme	20 Extreme
	3 Moderate	3 Low	6 Moderate	9 High	12 High	15 Extreme
	2 Minor	2 Low	4 Moderate	6 Moderate	8 High	10 High
	1 Negligible	1 Low	2 Low	3 Low	4 Moderate	5 Moderate

Example Quantitative Risk Matrix

Likelyhood	Consequences				
	Insignificant *Risk is easily mitigated by normal day to day process*	**Minor** *Delays up to 10% of Schedule Additional cost up to 10% of Budget*	**Moderate** *Delays up to 30% of Schedule Additional cost up to 30% of Budget*	**Major** *Delays up to 50% of Schedule Additional cost up to 50% of Budget*	**Catastrophic** *Project abandoned*
Certain *>90% chance*	High	High	Extreme	Extreme	Extreme
Likely *50% - 90% chance*	Moderate	High	High	Extreme	Extreme
Moderate *10% - 50% chance*	Low	Moderate	High	Extreme	Extreme
Unlikely *3% - 10% chance*	Low	Low	Moderate	High	Extreme
Rare *<3% chance*	Low	Low	Moderate	High	High

Risk Quantification

Quantification of risk generally necessary for informed risk decision-making; necessarily involves quantifying value of human life, which often seen as callous

- Intent not to value human life in moral sense, but rather to assign value to life (as with other loss categories) as means for making risk/benefit decisions
- Life value results from collective decision regarding balancing of social benefit and social risk
- Problem is to assign value to human life that reflects society's willingness to pay to avoid death from involuntary risk
- If value of life not quantified, resources (also having value) cannot be allocated rationally to develop and implement risk counter-measures to protect life
- If life given infinite value, no distinction can be made between resources justified to protect one life and those justified to protect many lives

Quantifying Human Life

To provide context as to what quantifying human life means, estimates for value of a statistical life (VSL) in Western countries typically range from $1 million to $10 million

- VSL is cost estimate for reducing average number of deaths by one
- U.S. government does not have official VSL threshold; different agencies use different values
  - Office of Management and Budget, $7 – 9 million (2012)
  - Environmental Protection Agency, $9.1 million (2010)
  - Food and Drug Agency, $7.9 million (2011)
  - Dept. of Transportation, $9.6 million (2016)
  - Federal Emergency Management Agency, $7.5 million (2020)

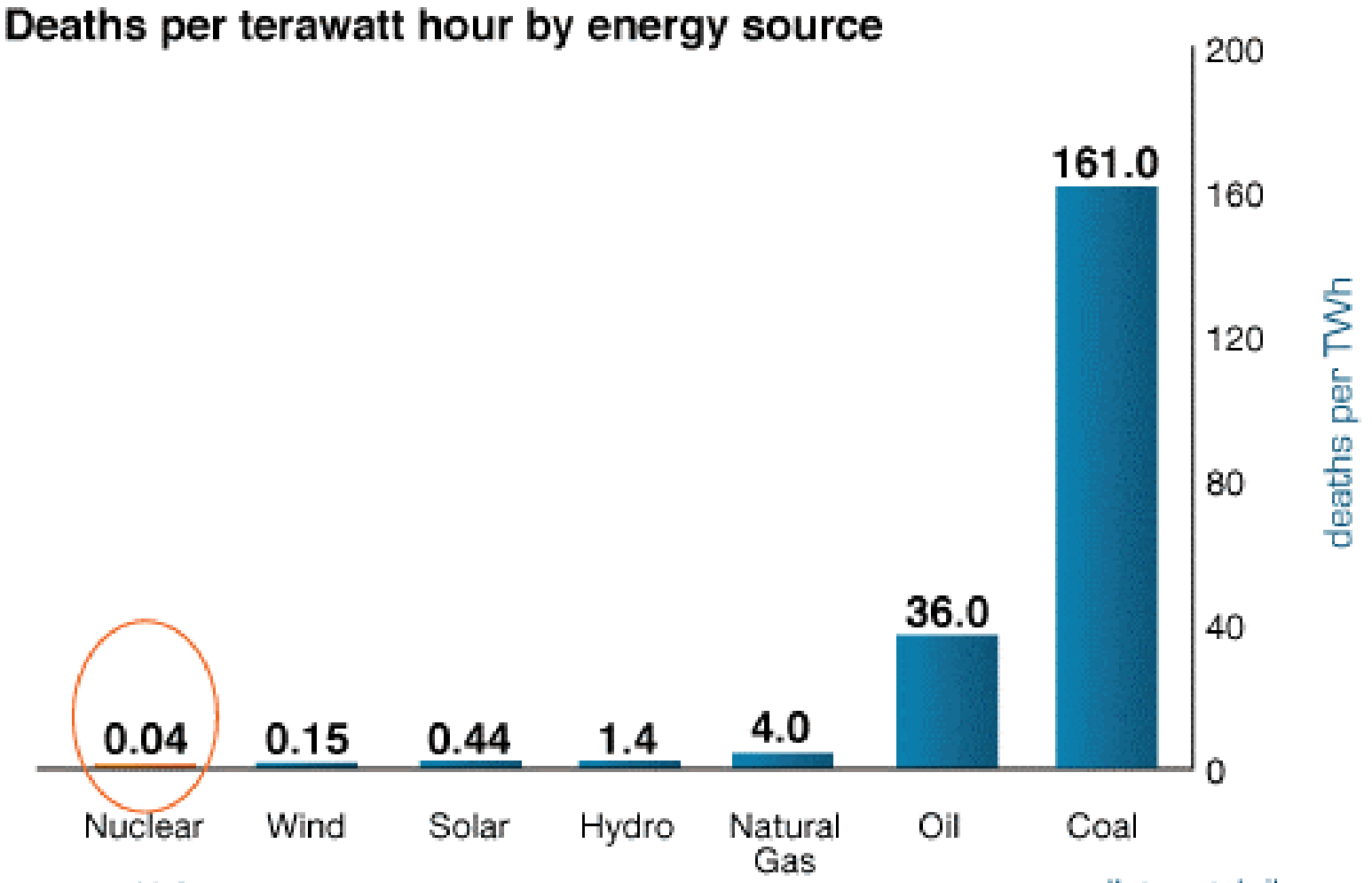
Risk Acceptability

- Biggest stumbling block – who has authority to establish what risk is acceptable
- Determining what constitutes acceptable level of risk seldom without controversy
  - Acceptance level will vary depending on one's perspective regarding risk under discussion
  - Will never be consensus
  - Generally determined by what individuals or societies willing to accept or tolerate
    - in exchange for perceived benefits, or
    - to avoid taking undesired mitigation measures or costly protective measures
  - Sometimes determined by least objectionable option in decision-making activity where some form of action is necessary

Nuclear Power Plant Risk

- Perception of nuclear power as uniquely dangerous reflected in regulatory burden placed on nuclear industry
  - Safety approach unnecessarily geared towards “as low as possible” philosophy, exhibited by application of both linear no-threshold (LNT) dose-response model and as-low-as-reasonably-achievable (ALARA) principle
  - Continual ratcheting down of worker radiation exposure levels with no observable health benefit sends incorrect message regarding radiation risk
  - Inadequate consideration of how inappropriate decisions regarding nuclear power plant risk creates greater risks elsewhere (e.g., lifecycle toxic wastes from using alternate energy resources)
- When entire energy resource lifecycle taken into account, nuclear power plant safety record unmatched by any other energy source (next slide graphic)

Nuclear: The Safest Energy Source of All

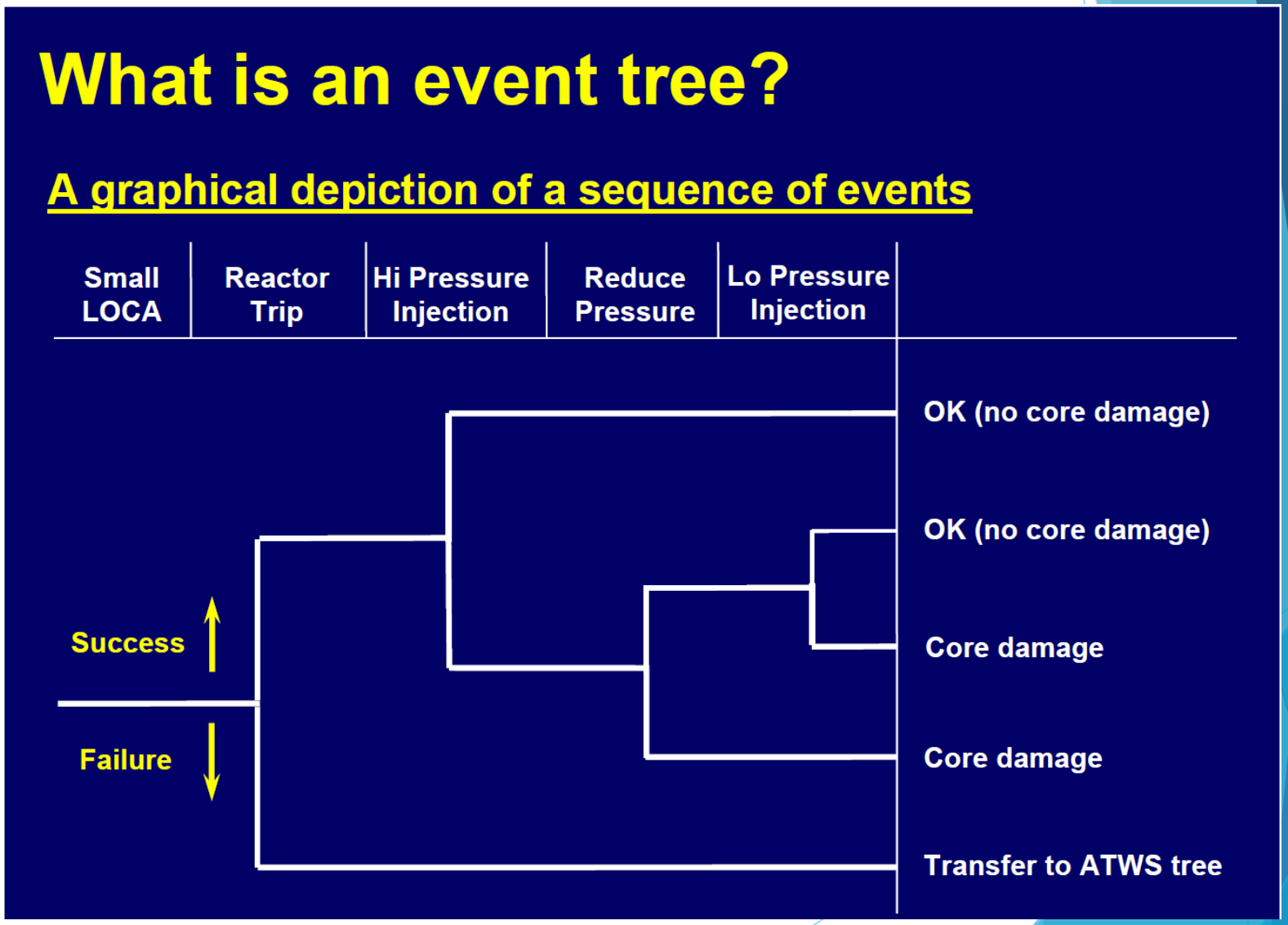


Evaluation of Nuclear Power Plant Risks

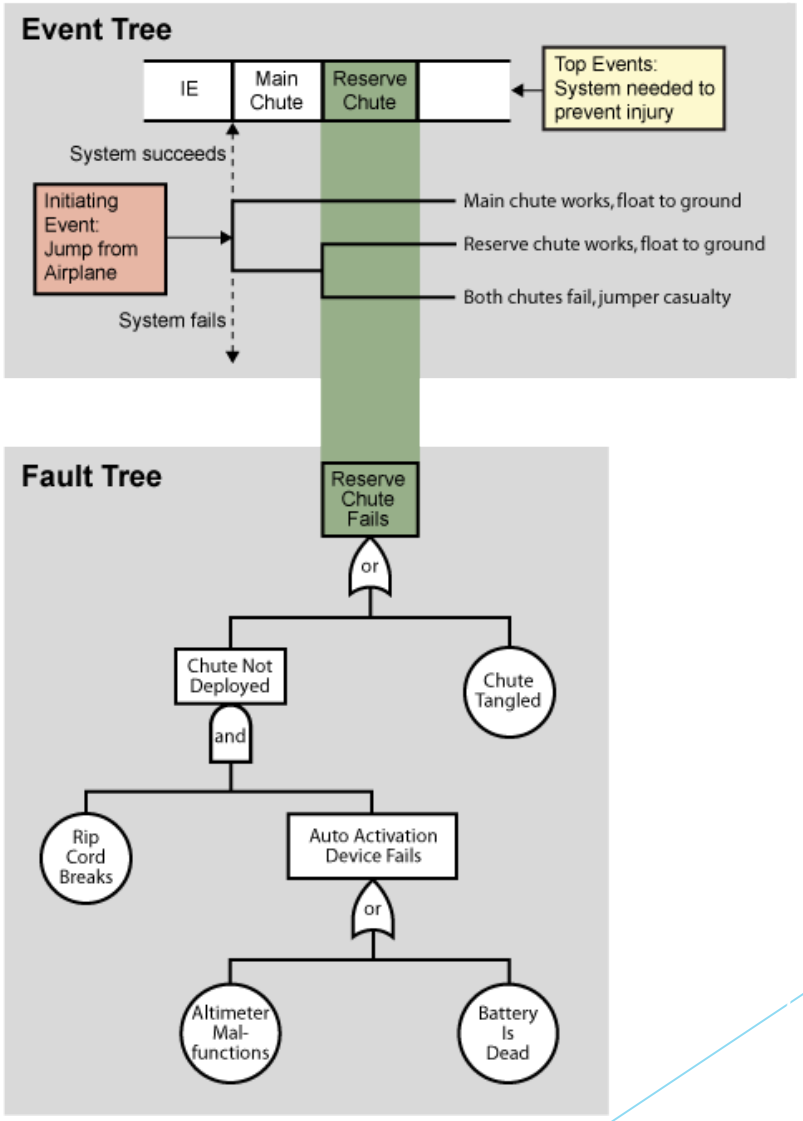
Nuclear power plant risks evaluated by performing probabilistic risk assessments (PRA)

- Performed to provide systematic assessments of public risk associated with operation of nuclear power reactors
- Use event trees and fault trees to identify and analyze power plant initiating events, safety function performance, and accident sequences to assess probability and consequences of not achieving safe, stable accident outcomes
- PRA outputs include estimates of
  - reactor core damage frequency
  - radiological release frequencies
  - radiological consequences to public

Example Event Tree



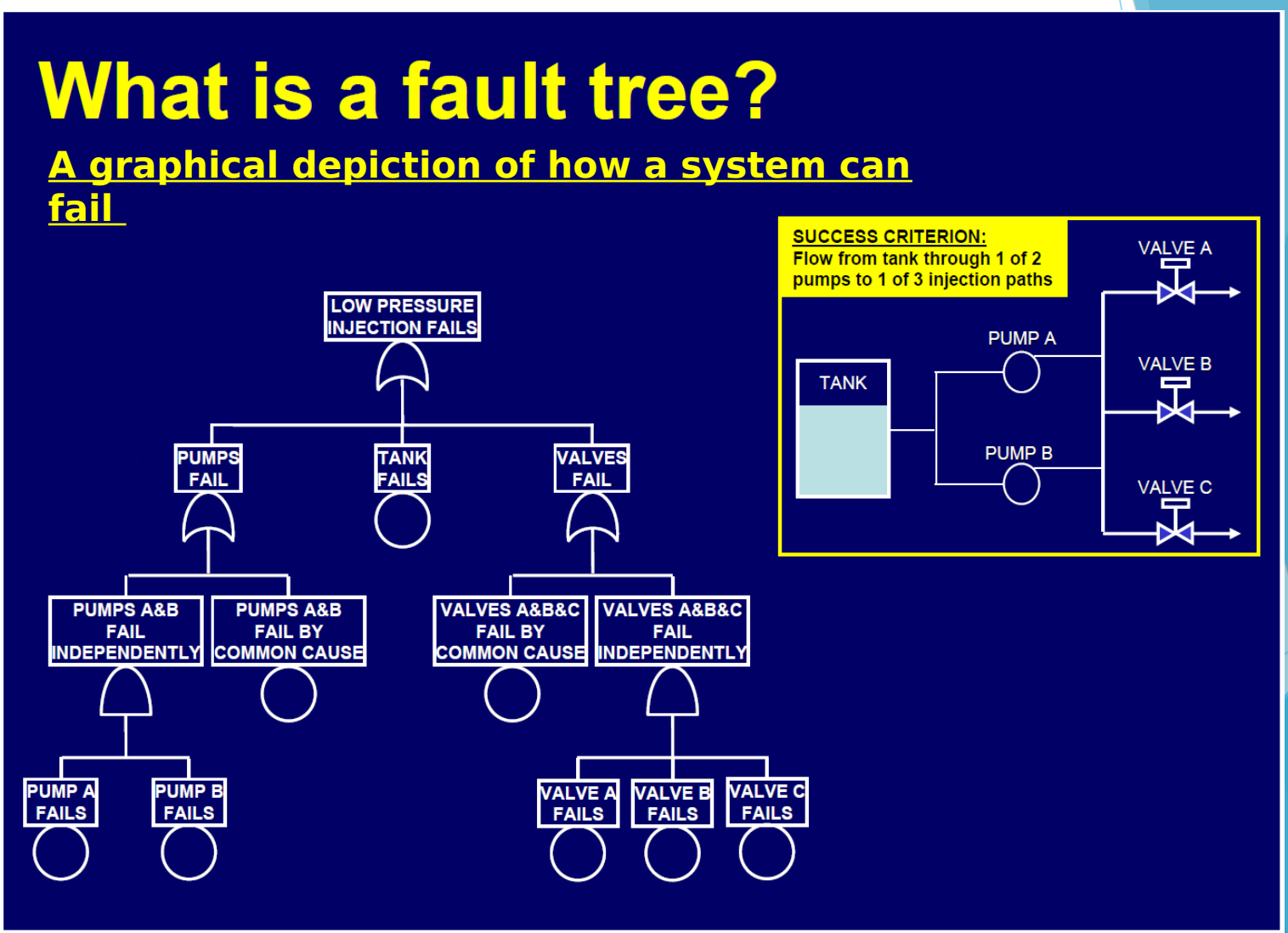
Event Tree-Fault Tree Relationship



Example Fault Tree

What is a fault tree?

A graphical depiction of how a system can fail



SIMPLY CODING

Boolean Algebra

AND

Input A	Input B	Output
0	0	0
0	1	0
1	0	0
1	1	1

A AND B, A.B, A ∧ B

NOT

Input A	Output A'
0	1
1	0

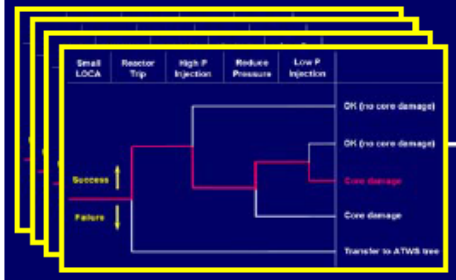
NOT A, ~A, A′, Ā

OR

Input A	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	1

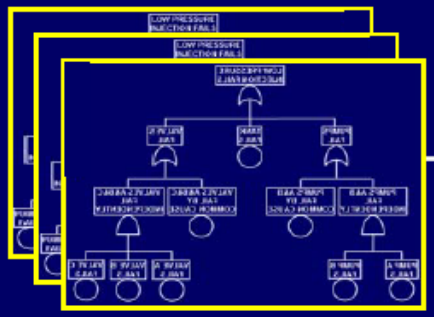
A OR B, A+B , A ∨ B

How do we "solve" the PRA model?



CORE DAMAGE SEQUENCES:

- Small LOCA OCCURS & Reactor Trip SUCCEEDS & High Pressure Injection FAILS & Reducing Pressure SUCCEEDS & Low Pressure Injection FAILS
- … (may be several on each tree!)

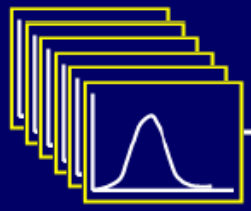


SYSTEM CUTSETS:

- PUMP A FAILS & PUMP B FAILS
- TANK FAILS
- … (may be several for each tree!)

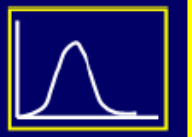
CORE DAMAGE CUTSETS:

- SMALL LOCA & HPI TANK FAILS & LPI PUMP A FAILS & LPI PUMP B FAILS
- SMALL LOCA & HPI PUMP A FAILS & HPI PUMP B FAILS & LPI TANK FAILS
- … (many combinations per sequence!)



FAILURE PROBABILITIES & INITIATING EVENT FREQUENCIES

- CORE DAMAGE FREQUENCY
- UNCERTAINTY ANALYSIS
- IMPORTANCE MEASURES
- SENSITIVITY STUDIES
- RISK INSIGHTS



Sources of PRA Input Data

Frequency of occurrence and failure probability data comes from

- Operating experience
  - Frequency of initiating events
  - Failure rates of plant equipment
  - Equipment repair and recovery probabilities
- Expert elicitation - provides likelihood information for rare event occurrences
- Human reliability analysis – provides information regarding likelihood of human errors
- Common cause failure modeling – provides additional insight into dependent system/component failure probabilities

Sources of PRA Input Data (cont.)

- Example operating experience databases
  - Reliability and Availability Data System (US Nuclear Regulatory Commission)
  - ASM Failure Analysis Database (ASM International)
  - Process Equipment Reliability Database (Center for Chemical Process Safety)
  - IEEE Standard 500-1984 Reliability Data for Pumps and Drivers, Valve Actuators, and Valves

Sources of PRA Input Data (cont.)

- Example human reliability databases
  - Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (NUREG/CR-1278)
  - The Scenario Authoring, Characterization, and Debriefing Application (SACADA) Database for Human Reliability and Human Performance (U.S. Dept. of Energy, Office of Scientific and Technical Information)
  - The Nuclear Computerized Library for Assessing Reactor Reliability (U.S. Nuclear Regulatory Commission)
- Common-Cause Failure Database and Analysis System (NUREG/CR-6268)

PRA Accident Consequences

PRAs use probabilistic risk models developed from reactor safety studies to assess potential accident consequences

- Assume conservatively high radioactive material releases under severe accident conditions
- Apply linear no-threshold (LNT) dose-response and collective-dose models for predicting cancer risk fatalities
  - Flawed nature of LNT model extensively addressed by Dr. Edward Calabrese
  - Use of collective-dose model for predicting radiation-induced fatalities rejected by American Health Physics Society

Scope of PRA Accidents

- Range of PRA limited to Design Basis Accidents
  - Credible operational or non-operational events for which protective, preventive, and mitigative safety measures provided in plant design
  - DBAs establish domain of acceptable performance requirements for plant structures, systems, and components, such that accident occurrence will not endanger health and safety of plant personnel or general public
- PRA defines nuclear power plant risk envelope

Design Basis Accident General Event Characterizations

- Overcooling – increase in secondary-side heat removal
- Undercooling – decrease in secondary-side heat removal
- Overfilling – increase in reactor coolant inventory
- Loss of coolant flow – decrease in reactor coolant system flow rate
- Loss of coolant – decrease in reactor coolant inventory

Design Basis Accident
General Event Characterizations (cont.)

- Reactivity excursion – core reactivity and power anomalies (events that cause undesired increases in fission rate)
- Anticipated transient without reactor scram – reactivity excursion without reactor shutdown by rapid insertion of control rods
- Spent fuel/radioactive waste system release – radioactivity release from spent fuel assembly or waste handling subsystem or component

Design Basis Accident
General Event Characterizations (cont.)

- External event – natural or human-caused events that can affect plant operating and safety systems
  - Natural events include phenomena such as floods, hurricanes, tornadoes, earthquakes, and tsunamis
  - Non-natural events include aircraft impacts and nearby industrial explosions

PRA Risk Acceptance

- U.S. Nuclear Regulatory Commission specifies minimum acceptable nuclear power plant risk in terms of Safety Goals (aka Quantitative Health Objectives)
- Numerical values of minimum risks for prompt and latent cancer fatalities from accidental releases of radioactivity to offsite population established by NRC to be very small fraction (0.1%) of rates for prompt fatalities and latent cancer fatalities in U.S. population at large
- Results of nuclear power plant PRAs must be in compliance with NRC Safety Goals

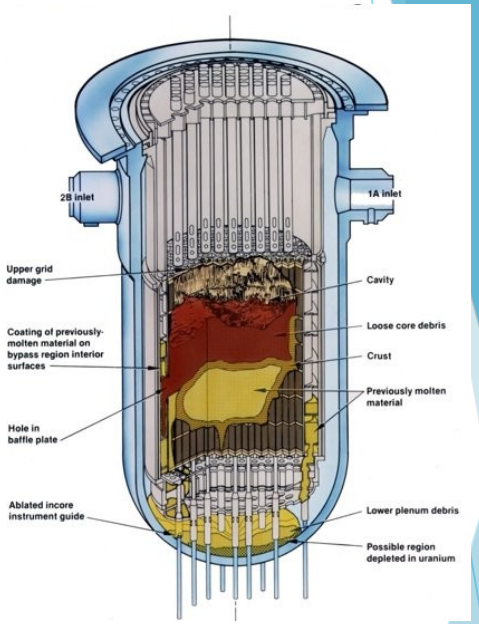
NRC Safety Goals for Operating Reactors

- Core Damage Frequency (CDF) < 10^{-4}/yr
  - 1 event in 10,000 years is surrogate for *latent cancer fatalities* (i.e., CDF x 0.1% < 10^{-7}/yr)
  - Cancer fatality risk to general U.S. population from all causes ≈ 2 x 10^{-6} per year*
- Large Early Release Frequency (LERF) < 10^{-5}/yr
  - 1 event in 100,000 years is surrogate for *prompt fatalities* (i.e., LERF x 0.1% < 10^{-8}/yr)
  - Prompt fatality risk to general U.S. population from all accidents ≈ 5 x 10^{-7} per year*

* Ref. George Apostolakis, Safety Goals and Risk-Informed Regulation at the U.S. NRC, January 13, 2014

NRC Safety Goals for New Reactors

Core Damage Frequency (CDF) < 10^{-5} /yr



Large Release Frequency (LRF) < 10^{-6} /yr

Assessment of NPP PRA Realism

Based on observations of Three Mile Island and Fukushima nuclear plant accidents

- Probability of occurrence of some accidents greater than assumed in plant PRAs
- Accident radiological consequences over-estimated (i.e., latent radiation-induced cancers over-estimated relative to actual observations – the LNT problem)
- Effects of unwarranted public evacuations more damaging to public health than radiation release from reactor core melt accident

State-of-the-Art Reactor Consequence Analysis

2012 State-of-the-Art Reactor Consequence Analysis (NUREG-1935) concluded that

- Existing nuclear power plant resources and procedures can stop an accident, slow it down, or reduce its impact before it can affect public health
- Even if accidents proceed uncontrolled, they take much longer to happen and release much less radioactive material than suggested by earlier analyses
  - Individual early fatality risk from selected important SOARCA scenarios is essentially zero
  - Individual latent cancer fatality risk from scenarios is thousands of times lower than NRC Safety Goal and millions of times lower than general cancer fatality risk in U.S. from all causes, even assuming linear no-threshold (LNT) dose-response model

Effect of Excessive PRA Conservatism

NUREG-1935 stated:

- Unrealistic estimations of public health consequences have driven many complex regulations for nuclear power plants to prevent very unlikely events that could release less than harmful amounts of radioactive material
- These regulations have hugely increased costs of nuclear power plant construction, operation, and maintenance

Nuclear Risk Communication – the Good, the Bad, and the Ugly

The Good

Following 1979 Three Mile Island media disaster, Peter Sandman and Vincent Covello developed and published guidance for how to effectively communicate risk to general public

Nuclear Risk Communication – the Good, the Bad, and the Ugly (cont.)

The Bad

Issue of nuclear risk communication a topic of discussion ever since, with seemingly no improvement in past 45+ years – why?

- Political anti-nuclear bias
- Media anti-nuclear bias
  - Promotes fear of all things nuclear
  - Establishes false narratives, including allegations of nuclear industry incompetence and accident coverups
  - Inhibits public education
- Public easily frightened of things they don't understand

Nuclear Risk Communication – the Good, the Bad, and the Ugly (cont.)

The Bad (cont.)

Primary damage from three nuclear industry accidents, loss of public trust in industry communications, very difficult to overcome

- American nuclear industry lost public's trust with mismanaged communications of 1979 Three Mile Island accident
- Anti-nuclear activists and media took advantage of attempted Russian coverup of 1986 Chernobyl accident
- Unwarranted mandatory evacuation of nearby hospitals and nursing homes following Fukushima accident led to unnecessary health-related deaths; unwarranted closure of nearby homes and businesses led to depression-induced suicides

Nuclear Risk Communication – the Good, the Bad, and the Ugly (cont.)

The Bad (cont.)

Underlying risk communication guidelines is implicit
assumption that “audiences” for which communication is intended are rational people capable of critical thinking

- People continue to demonstrate primary influence of beliefs is emotion, especially fear of unknown, not rational thinking
- Majority of Americans don’t know how to think critically about anything; public education system stopped teaching critical thinking skills long ago
- Public often parrots what they hear and reluctant to admit beliefs may be incorrect

Nuclear Risk Communication – the Good, the Bad, and the Ugly (cont.)

The Ugly

More often than not, emotions overwhelm facts, and lies take on life of their own

- Movement in today's public school system teach students how they feel about issues more important than the science
- Movement on college and university camp to shut down communications deemed to l politically-incorrect
- Censoring by media gatekeepers of communications alleged to be misinformat or disinformation

Even good risk communications doomed to failure in absence of rational thinking

Effect of Emotions and Groupthink in Communications

During periods of peace and prosperity, when the prevailing social mood is positive, it's often tough to know who is truly decent and reasonable. During times of stress and fear, people are far more inclined to show their true colors. Many get swept up in the emotions and groupthink of the frightened herd, thereby losing their capacity for critical thinking and principled action. Under such circumstances, if you insist on maintaining your individuality, you will likely be shocked to discover that even people whom you took to be old friends may join the herd in ostracizing you.*

* McCullough, Dr. P.A. and J. Leake, *The "Unvaccinated are Unclean" Compilation*, May 31, 2023

Public Unawareness and Indifference

When asked why so many people are so easily duped regarding discussions of energy and power, Distinguished Professor Emeritus Vaclav Smil replied, “There has never been such a depth of scientific illiteracy and basic innumeracy as we see today. Without any physical, chemical, and biological fundamentals, and with equally poor understanding of basic economic forces, it is no wonder that people will believe anything.”*

* Robert Bryce, *Elon’s Terrible, Horrible, No Good, Very Bad Battery Math*, April 7, 2023

The Issue of Beyond Design Basis Accidents

Beyond Design Basis Accidents

- Postulated operational or non-operational events for which no formal risk analysis and no specific risk mitigating measures required
- Characterized as potentially high consequence events having extremely low probability of occurrence
- Involve successive failures of multiple barriers provided for fission product retention
- Have potential to cause serious reactor core damage, including meltdown
- Have potential to cause public harm

BDBA Evaluation

No formalized analysis approach, but nuclear power plant accident documentation must

- demonstrate understanding of BDBA risk and address available risk controls
- address costs and benefits associated with BDBA risk mitigation
- address adequacy of plant's emergency preparedness plan for BDBA response
- show understanding of BDBA effects on safety
  equipment survivability

BDBA Risk Acceptance

Beyond Design Basis Accident risk acceptability hinges on two questions.

- What risk is society willing to accept for very low frequency events such as earthquakes and tsunamis; that is, is a one-in-500-year event acceptable? How about a one-in-100-year event?
- What maximum cost is society willing to incur to guarantee only “tolerable” plant damage from any conceivable risk (e.g., a meteor strike)?

If society is unwilling to tolerate very low probability risks, or bear the expense to bring all conceivable risks into a nuclear power plant’s design basis, then abundant and reliable electricity may, at some point, become an historical artifact.

Beyond Design Basis Accident?